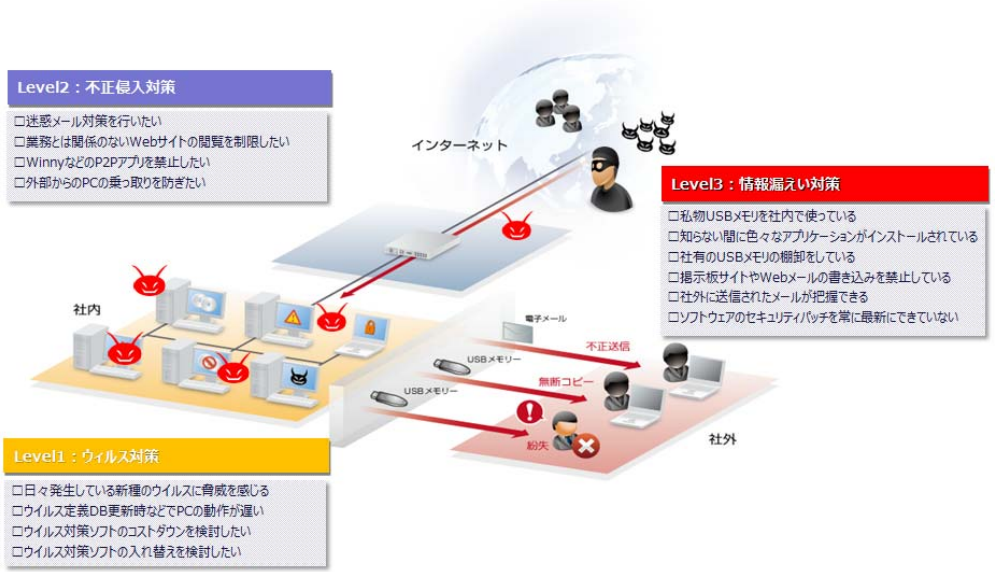
個人情報を守るために、安全管理措置の徹底を！

無料セキュリティ診断実施中

個人情報の漏えいを未然に防ぐために、お客様のオフィスに迫る危険をご確認して頂き、
安心安全なオフィスについてご説明させて頂きます。

情報セキュリティ対策　チェックシート　※１つでもあてはまるものがあれば対策をご検討下さい。



情報セキュリティ診断　※まずは、貴社のセキュリティ状況を把握しましょう。

外部からの攻撃数、
内部からの漏えいの
リスクを視覚化します！！

●お求めは信用のある当社で

エフ･ビー･エム株式会社
東京都千代田区飯田橋2-13-7
TEL:03-6272-3453
FAX:03-3230-1071

2017年12月現在

エフ･ビー･エム株式会社

〒102-0072　東京都千代田区飯田橋二丁目13番7号　三喜ビル

BUSINESS TREND NEWS

企業の大小によらず すべての事業者が 個人情報保護法の対象へ！

- 2017年5月30日
  改正個人情報保護法が施行
- 「個人情報保護委員会」が設立され
  事件が発生すると
  立ち入り検査や罰金適用のケースも
- 中小規模事業者が
  知っておくべきポイントを押さえ
  自社が個人情報を適切に
  管理しているかチェックしましょう

一人でも従業員がいたり、一件でも個人情報を扱うなら、中小規模事業者でも法の遵守が義務づけられることに！

2005年に個人情報保護法が全面施行されて十数年。スマートフォン、SNSなどの情報技術の発展とともに、中小規模事業者の皆様においても、個人情報を取り扱う業務の内容に変化が生じつつあるのではないでしょうか。また、漏えいによるプライバシー侵害の危険も増大。消費者の間でも不安が高まり、今までは取り扱う個人情報が5,000件以下の中小規模事業者については法の対象外であることに対し、疑問の声が挙がるようになりました。そこで、個人情報の利活用の促進と保護強化という二つの観点から対応を検討。この度、改正法が施行されることになりました。

ここに注目！ 主な改正のポイント

	改正前	改正後
① 対象範囲の拡大	・5,000件以上の個人情報の取り扱いがある事業者のみ	・1件でも個人情報を取り扱っていれば対象となる（すべての事業者が対象）
② 個人情報の定義の明確化	・個人情報＝特定の個人を識別することができる情報 ・他の情報と容易に照合することができ、それにより特定の個人を識別することができるもの（個人情報とひもづく移動履歴や購買履歴）	・「個人識別符号」が新たに対象に ① 生体認証に用いられるデータ（身体の一部の特徴を電子計算機のために変換した符号） DNA、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋 ② サービス利用や書類において対象者ごとに割り振られる符号 公的な番号旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー、各種保険証等 ・「要配慮個人情報」が新設　本人の人種、信条、病歴、犯罪の経歴など
③ 監督機関の新設	・業種ごとに所轄省庁やガイドランが異なる	・「個人情報保護委員会」に権限を一元化。立入検査権がある。
④ 第三者提供の制限	・名簿の転売ルートをトレースできなかった ・顧客情報データベースから不正に持ち出しても、個人情報保護法上の刑事罰がなかった	・確認記録作成等を義務化（トレーサビリティを確保。第三者提供についての記録・説明義務） ・「個人情報データベース提供罪」の新設

事業者（提供）：記録の作成・保存義務　提供の年月日、受領者の氏名等の記録・保存
個人情報 → 第三者提供
事業者（受領）：確認、記録の作成・保存義務　提供者の氏名、取得経緯等を確認　提供の年月日、確認事項等を記録保存

万が一のリスク もしも情報が漏えいしたら・・・

たった一度でも情報漏えいを起こしてしまうと、取引先からの信用低下は免れず、補償金などの支払いも発生するリスクがあります。情報の紛失・盗難や不正アクセスなど、原因となるリスクを的確に把握し、対策に努めて、情報漏えいを防ぎましょう。

会社の信頼低下

罰則あり

○国からの命令に違反した場合
⇒6ヶ月以下の懲役又は30万円以下の罰金

○虚偽の報告等をした場合
⇒30万円以下の罰金

○従業員等が不正な利益を図る目的で個人情報データベース等を提供、又は、盗用した場合
（個人情報データベース等不正提供罪）
⇒1年以下の懲役又は50万円以下の罰金

【身近な事例】

CASE 1 **銀行員の家族が芸能人の個人情報をツイート**
銀行員の母親が業務上知り得た芸能人たちの個人情報を娘に漏らし、ツイートにより流出。重大な個人情報漏えい事件としてTwitterが炎上し、銀行が謝罪する事態に。

CASE 2 **教諭が置き忘れた学級名簿がLINEで流出**
教諭が校内に置き忘れた新年度の学級編成用の生徒名簿を生徒が発見。スマートフォンで撮影した上、LINEで複数の同級生に送信したことが保護者からの指摘で発覚。

中小規模事業者が個人情報保護法改正ですべきこと！

準備 個人情報を取り扱う者が複数いる場合、責任者を任命（経営者）

情報漏えい発生時に備えて責任者を任命し、従業員からの報告連絡体制をあらかじめ確認。責任者は年に1回会議を開くなど、取り扱い状況を定期的に点検しましょう。

取得 情報を何に使うか、目的を決めて、本人に伝える（担当者）

企業が個人情報を利用する際は、あらかじめ利用目的を特定する必要があります。そして、情報取得時に本人に伝えるか、あらかじめホームページや店頭での掲示などで公表してください。

※ただし、例えば名刺交換をした場合など、情報の利用目的が明らかな場合は、逐一相手に伝える必要はありません。

利用提供 決めた目的以外に利用したり、他人に渡す際は本人の同意を得る（担当者）

取得した個人情報は、あらかじめ公表または同意を得た利用目的の範囲内でしか使えません。したがって、個人情報の取得にあたっては、何に使うかという利用目的をしっかりと考えた上で本人に伝えましょう。もし、すでに取得した個人情報を特定の目的以外のことに利用したり、他人に渡す場合には、あらかじめ本人の同意を得てください。

保管・安全管理措置 安全に管理する（担当者）

個人情報を取り扱う事業者は、下記のような安全管理措置を施す必要があります。
・個人情報を取り扱う部屋の入退室管理等
・個人情報を取り扱うパソコンをセキュリティーワイヤーで固定
・パソコンのID/パスワード設定、ウイルス対策
・紙の名簿は施錠できるキャビネットで保管など、情報が漏えいしないような措置を検討しましょう。

開示 本人からの請求（開示や訂正など）に応じる（担当者）

保有している個人情報について、本人から開示や訂正等を請求されたら、企業は対応しなければなりません。また、利用目的を問われた場合もしっかり答えられるようにしておきましょう。

レベルに応じたセキュリティ対策

企業の情報セキュリティ対策はどこまで必要か。
さまざまな要因による情報漏えいや、マルウェア感染により被害者でありながら加害者となることで、社会的信用を失わないためレベルに応じた対策が必要です。

ITの実装 Level.1
社内パソコンのウイルス対策を実施する。

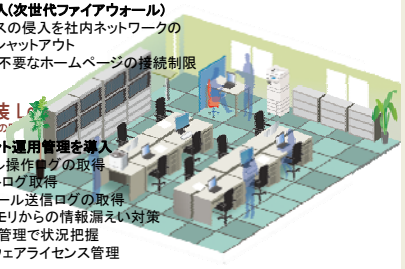
企業向けウイルス対策ソフトの導入
－ 全社のウイルス対策ソフトを一元管理

ITの実装 Level.2
社内ネットワークの不正侵入対策を実施する。

UTMを導入（次世代ファイアウォール）
－ ウイルスの侵入を社内ネットワークの水際でシャットアウト
－ 業務上不要なホームページの接続制限

ITの実装 L
社内パソコンの

クライアント運用管理を導入
－ ファイル操作ログの取得
－ プリントログ取得
－ 電子メール送信ログの取得
－ USBメモリからの情報漏えい対策
－ IT資産管理で状況把握
－ ソフトウェアライセンス管理



詳しくは 国の行政機関「個人情報保護法質問ダイヤル（個人情報保護委員会）」 電話番号 03-6457-9849　受付時間 土日祝日および年末年始を除く 9:30～17:30